UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/801,363	03/15/2004	Jochen Weber	10191/3602	3174

26646 7590 06/15/2009

KENYON & KENYON LLP
ONE BROADWAY
NEW YORK, NY 10004

EXAMINER	
TRAORE, FATOUMATA	
ART UNIT	PAPER NUMBER
2436	

MAIL DATE	DELIVERY MODE
06/15/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/801,363	WEBER ET AL.	
	Examiner	Art Unit	
	FATOUMATA TRAORE	2436	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *06 March 2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-8,10-16 and 18-24* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-8,10-16 and 18-24* is/are rejected.

7)☒ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This is in response to the amendment filed March 6, 2009. Claims 1 and 10 have been amended. Claims 9 and 17 have been cancelled. Claims 20-24 have been added. Claims 1-8, 10-16 and 18-24 are pending and have been considered below.

Response to Arguments

2. Applicant amended claims 1 and 10 and added new claim 20 and presented argument with respect to the newly amended claims. Applicant's argument has been fully considered. However, upon further consideration, a new ground(s) of rejection is made in view of Ansell et al US 6,792,113

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1-3, 10-12, 20 and 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Brookner (US 7,308,718) in view of Ansell et al (US 6,792,113).

Claims 1 and 10: Brookner discloses a microprocessor system (Fig, 1) and a method for detecting an exchange of a module comprising:

i. a plurality of modules including a microprocessor and at least one storage module for storing code and data for the microprocessor, at least one of the

modules storing a serial number of the at least one module in a non-exchangeable manner(Fig. 1)

ii. an arrangement for storing a code number (herein after *encrypted serial number*) obtained from the serial number by using an encryption method (*RSA mythology*), and for storing information (*public which is used to decrypt the encrypted serial number*) calculate the serial number from the code number(*the aforementioned configuration request by system 105 includes information concerning (a) system public key 125 and (b) serial number 129 which is encrypted using system private key 127 in accordance with the RSA methodology) column 4, lines 1-15);*

iii. wherein the microprocessor is adapted to calculate a serial number from the code number on the basis of the information (*processor 133 at step 311 decrypts the encrypted serial number in the request using received system public key 125 0r alternatively the matching system public key in field 203 of the record) (column 4, lines 20-26),* to compare the calculated serial number to the stored serial number, and to execute or not execute at least part of the code as a function of a result of the comparison *(processor 133 at step 314 determines whether the resulting serial number matches that in field 205 of the record. If they do not match Otherwise, if they match, processor 133 at step 320 reads from field 207 of the record the identifiers indicating the software options specified by the user for installation in system 105) (column 4, lines 26- 40);*

iv. detecting an exchange *of the module if the serial number of the module does not match the decrypted serial number (If they do not match, processor 133 at step 317 denies the configuration request) column 26-40).*

Brookner does not explicitly discloses wherein at least two of the modules are each identified by a serial number, and the code number is obtained by encrypting a linking of the serial numbers of the at least two of the modules. However, Ansell et al disclose an adaptable security mechanism for preventing unauthorized of digital data, which further discloses wherein at least two of the modules are each identified by a serial number, and the code number is obtained by encrypting a linking of the serial numbers of the at least two of the modules(column 6, lines 5-20). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the teaching of Brookner such to produce the code number by encrypting a linking of the sat least two of the module. One would have been motivate to do so in order to provide the protection of digital data from unauthorized access as taught by Ansell et al.

Claims 2 and 11: Brookner and Ansell et al disclose a microprocessor system(Fig, 1) and a method for detecting an exchange of a module as in claims 1 and 10 above, and Brookner further discloses wherein the encryption method is asymmetrical (*RSA methodology) (column 3, line 50 to column 4, line 2*), the code number is calculated from the serial number with the aid of a secret key *(herein after private key*), and the information includes a public key as well as a program code for calculating the serial number from the code number (*serial number which is encrypted which is encrypted*

using system private key in accordance with the RSA methodology) (column 4, lines 10-14).

Claims 3 and 12: Brookner and Ansell et al disclose a microprocessor system(Fig, 1) and a method for detecting an exchange of a module as in claims 2 and 10 above, Ansell et al further disclose wherein one of the at least one module identified by the serial number is a storage module. However, Gammie discloses a security module, which further discloses wherein one of the at least one module identified by the serial number is a storage module (*Fig. 7, items 711, 716, 717, 712*). column 6, lines 5-20). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the teaching of Brookner such to identify a storage module by a serial number. One would have been motivate to do so in order to provide the protection of digital data from unauthorized access as taught by Ansell et al.

Claim 20: Brookner and Ansell et al disclose a microprocessor system(Fig, 1) as in claim 1 above, and Ansell et al further disclose wherein each of the modules is identified by a serial number, and the code number is obtained by encrypting a linking of the serial number of the each of the modules(column 6, lines 5-20).

Claim 21 Brookner and Ansell et al disclose a microprocessor system*(Fig, 1)* as in claim 1 above, and Ansell et al further disclose wherein the microprocessor is adapted to calculate a linking of the serial numbers of the at least two modules from the code number on the basis of the information(*column 6, lines 5-20*), And Brookner further discloses a step of to compare the calculated serial number to the stored linking of the serial numbers of the at least two modules *(column 4, lines 26- 40)*.

5. Claims 4, 5, 13, 14 , 23 and 24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Brookner (US 7,308,718) in view of Ansell et al (US 6,792,113) in further view of Gilley et al (US 5,771,287).

Claims 4 and 13 Brookner and Ansell et al disclose a microprocessor system (Fig, 1) and a method for detecting an exchange of a module as in claims 3 and 12 above, while either of them explicitly discloses wherein the code number is stored in a same storage module as the serial number. However Gilley et al discloses a microprocessor and method for controlling the feature set of a programmable device ,which further discloses wherein the code number is stored in a same storage module as the serial number (*the read only memory contains the serial, the code to enable the scrambling function) (column 6, lines 53-57 and Figure 1)*. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the combined teaching of Brookner and Ansell et al such to store the code number and the serial in the same storage module. One would have been motivate to do so in order to avoid the cost and time of replacing hardware to change the feature set (column 3, lines 25-45).

Claims 5 and 14: Brookner and Ansell et al disclose a microprocessor system (Fig, 1) and a method for detecting an exchange of a module as in claims 3 and 12 above, and Brookner further discloses wherein the storage module is an electrically rewritable, non-volatile memory (Fig. 1). while either of them explicitly disclose if the calculated and the stored serial numbers do not match includes a command for deletion of the storage module. However, Gilley et al discloses a microprocessor and method for controlling the

feature set of a programmable device ,which further discloses the code to be executed if the calculated and the stored serial numbers do not match includes a command for deletion of the storage module (*If the two authentication codes match, the programmable device will authorize to function with the present feature set by the present operation mode code. If they do not match, the programmable takes a number of different actions, including refusing to conduct certain functions, refusing to operate at all, or defaulting to a lower feature set, other action are possible (deletion of storage module))(column 4, lines 26-34)*. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the combined teaching of Brookner and Ansell et al such to delete the storage module if the calculated and the stored serial numbers do not match. One would have been motivate to do so in order to avoid the cost and time of replacing hardware to change the feature set (column 3, lines 25-45).

Claim 23: Brookner discloses a microprocessor system (Fig, 1), comprising:

i. a plurality of modules including a microprocessor and at least one storage module for storing code and data for the microprocessor, at least one of the modules storing a serial number of the at least one module in a non-exchangeable manner(Fig. 1)

ii. an arrangement for storing a code number (herein after *encrypted serial number*) obtained from the serial number by using an encryption method (*RSA mythology*), and for storing information (*public which is used to decrypt the encrypted serial number*) calculate the serial number from the code number(*the aforementioned configuration request by system 105 includes information*

concerning (a) system public key 125 and (b) serial number 129 which is encrypted using system private key 127 in accordance with the RSA methodology) column 4, lines 1-15);

iii. wherein the microprocessor is adapted to calculate a serial number from the code number on the basis of the information (*processor 133 at step 311 decrypts the encrypted serial number in the request using received system public key 125 0r alternatively the matching system public key in field 203 of the record) (column 4, lines 20-26),* to compare the calculated serial number to the stored serial number, and to execute or not execute at least part of the code as a function of a result of the comparison *(processor 133 at step 314 determines whether the resulting serial number matches that in field 205 of the record. If they do not match Otherwise, if they match, processor 133 at step 320 reads from field 207 of the record the identifiers indicating the software options specified by the user for installation in system 105) (column 4, lines 26- 40);*

iv. detecting an exchange *of the module if the serial number of the module does not match the decrypted serial number (If they do not match, processor 133 at step 317 denies the configuration request) column 26-40).*

Brookner does not explicitly discloses wherein at least two of the modules are each identified by a serial number, and the code number is obtained by encrypting a linking of the serial numbers of the at least two of the modules. However, Ansell et al disclose an adaptable security mechanism for preventing unauthorized of digital data, which further discloses wherein at least two of the modules are each identified by a serial number, and

the code number is obtained by encrypting a linking of the serial numbers of the at least two of the modules(column 6, lines 5-20). While neither of them explicitly discloses wherein the information required to calculate the serial number from the code number is stored in a different storage module than the code number, the different storage module being connected to the microprocessor in a non-separable manner. However, Gilley et al discloses a method for secure control of feature of a programmable device, which further disclose wherein the information required to calculate the serial number from the code number is stored in a different storage module than the code number, the different storage module being connected to the microprocessor in a non-separable manner(Fig. 1). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the teaching of Brookner such to produce the code number by encrypting a linking of the sat least two of the module. One would have been motivate to do so in order to provide the protection of digital data from unauthorized access as taught by Ansell et al. The motivation of connecting the different storage module to the microprocessor in a non-separable manner would have been to reduce the cost of manufacturing as taught by Gilley et al (column 1, lines 25-35).

Claim 24: Brookner , Ansell et al and Gilley et al disclose a microprocessor system as in claim 23 above, and Gilley et al further disclose wherein the different storage module and the microprocessor are integrated in a one-chip microprocessor(Fig. 1).

6. Claims 6-8, 15 and 16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Brookner (US 7,308,718) in view of Ansell et al (US 6,792,113) in further view of Lee et al (US 5,774,544).

Claims 6 and 15::Brookner and Ansell et al disclose a microprocessor system (Fig, 1) and a method for detecting an exchange of a module as in claims 1 and 10 above, while neither of them explicitly disclose wherein one of the at least one module identified by the serial number is the microprocessor. However, Lee et al discloses a microprocessor and a method for encrypting and decrypting serial number, which further discloses wherein one of the at least one module identified by the serial number is the microprocessor(*column 2, lines 5-20)*. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the combined teaching of Brookner and Ansell et al such as to identify the microprocessor by a serial number. One would have been motivate to do so in order to prevent reading of the serial the serial number taught by Lee et al.

Claims 7 and 16: Brookner and Ansell et al disclose a microprocessor system (Fig, 1) and a method for detecting an exchange of a module as in claims 1 and 10 above, while neither of them explicitly discloses wherein the information required to calculate the serial number from the code number is stored in a different storage module than the code number. However, Lee et al discloses a microprocessor and a method for encrypting and decrypting serial number, which further discloses wherein the information required to calculate the serial number from the code number is stored in a different storage module than the code number (*Fig. 4b)*. Therefore, it would have been obvious to one having

ordinary skill in the art at the time the invention was made to modify the teaching of Brookner and Ansell et al such as to store the code number and the serial number in different storage module. One would have been motivate to do so in order to prevent reading of the serial the serial number taught by Lee et al.

Claim 8:Brookner and Ansell et al disclose a microprocessor system (Fig, 1), as in claim 7 above, and Lee et al further discloses wherein the different storage module is connected to the microprocessor in a non-separable manner (*Fig. 1*).

7. Claims 18, 19 and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Brookner (US 7,308,718) in view of Ansell et al (US 6,792,113) in further view of Osborn (US 6,026,293).

Claim 18: Brookner and Ansell et al disclose a method for detecting an exchange of a module as in claim 10 above, while neither of them explicitly discloses wherein steps of the method are executed upon each start-up of the microprocessor system. However, Osborn discloses an apparatus for preventing electronic memory tampering, which further discloses that the steps of the method are executed upon each start-up of the microprocessor system (*a process for telephone power up and memory validation for the system depicted in Fig 4, according to an exemplary embodiment of the invention, is illustrated in Fig 5. After the cellular telephone is turned on, boot code within the Internal Read Only Memory, (IROM) is executed by the microprocessor to initialize the controller. Has code containing in the IROM is then run to perform an audit hash value calculation over selected contents of the flash program and the Electronic Serial Number*

(ESN) value stored in EEPROM) (column 8, lines 19-30). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the combined teaching of Brookner and Ansell et al such as to add the steps of execution of the method at each start-up. One would have been motivate to do so in order to prevent unauthorized manipulation of desirably secure memory contents in an electronic device taught by Osborn.

Claims 19 and 22: Brookner and Ansell et al disclose a microprocessor system (Fig, 1), and a method for detecting an exchange of a module as in claims 1 and 10 above, wherein steps of the method are periodically executed during operation of the microprocessor system. However, Osborn discloses an apparatus for preventing tampering with memory in electronic device, which further discloses that steps of the method are periodically executed during operation of the microprocessor system (a periodic hash value calculation process is enabled, where after the cellular telephone begins normal operation) (column 8, lines 38-40). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to modify the teaching of Brookner such as to add the steps of a periodical execution of the method. One would have been motivate to do so in order to prevent unauthorized manipulation of desirably secure memory contents in an electronic device as taught by Osborn.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Fatoumata Traore whose telephone number is (571) 270-1685.

The examiner can normally be reached Monday through Thursday from 7:00 a.m. to 4:00 p.m. and every other Friday from 7:30 a.m. to 3:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nassar G. Moazzami, can be reached on (571) 272 4195. The fax phone number for Formal or Official faxes to Technology Center 2100 is (571) 273-8300. Draft or Informal faxes, which will not be entered in the application, may be submitted directly to the examiner at (571) 270-2685.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the Group Receptionist whose telephone number is (571) 272-2100.

Thursday, June 11, 2009

/F. T./

Examiner, Art Unit 2436

/Nasser G Moazzami/

Supervisory Patent Examiner, Art Unit 2436